This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method of restoring data of a key-server in communication with a communication network comprising:

providing the key-server for storing secure electronic keys, the key-server in communication with the communication network;

providing to at least a computer in communication with the communication network, a plurality of portable data storage devices each having stored thereon secure electronic key data relating to a single authorized user; and,

copying from each of the plurality of portable data storage devices for storage in the key-server, secure electronic key data relating to the single authorized user.

2. (Previously Presented) A method of restoring data of a key-server in communication with a communication network as defined in claim 1 wherein the step of copying comprises:

forming a secure communication session between at least one of the plurality of portable data storage devices and the key-server;

transferring the secure electronic key data via the secure communication session from the portable data storage device to the key-server; and,

storing the transferred secure electronic key data within memory means of the ey-server.

3. (Previously Presented) A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the plurality of portable data storage devices comprise all the secure electronic key data to be restored in the key-server.

4. (Previously Presented) A method of restoring data of a key-server in communication with a communication network as defined in claim 3 wherein the plurality of

portable data storage devices includes memory having stored therein secure electronic key data relating to each single authorized user of the communication network.

5. (Previously Presented) A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the portable data storage device includes a processor for ciphering data using the secure electronic key data stored therein and comprising:

providing cryptographic functions within the portable data storage device using the secure electronic key data stored therein.

6. (Previously Presented) A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the key-server includes a processor for ciphering data using the secure electronic key data stored therein and comprising:

providing cryptographic functions within the key-server using the secure electronic key data stored therein.

7. (Previously Presented) A method of restoring data of a key-server in communication with a communication network as defined in claim 6 comprising:

determining at least an available user information entry device from a plurality of known user information entry devices;

receiving unique user identification information via the at least an available user information entry device; and,

registering the received user identification information against security data for that user stored in the key-server;

wherein, when the user identification information is indicative of an authorized user ciphering data is performed with secure electronic key data associated with the authorized user.

8. (Original) A method of restoring data of a key-server in communication with a communication network as defined in claim 3 wherein each of the plurality of portable data storage devices are provided at each of a plurality of computers in communication with the network.

9. (Original) A method of restoring data of a key-server in communication with a communication network as defined in claim 8 wherein the portable data storage device is one of a token and a smart card.

10. (Original) A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the portable data storage device is one of a token and a smart card.

11. (Original) A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein at least a portable data storage device provides dedicated cryptographic functions for the at least a computer in communication with the communication network using the security data stored internal to the at least a portable data storage device.

12. (Original) A method of restoring data of a key-server in communication with a communication network as defined in claim 11 wherein the security data stored internal to the at least a portable data storage device are not accessible in a useable form from outside of the key-server and the at least a portable data storage device.

13. (Original) A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the key-server provides dedicated cryptographic functions for the at least a computer in communication with the communication network using the security data stored internal to the key-server.

14. (Previously Presented) A method of backing up data of a key-server in communication with a communication network comprising:

providing the key-server in communication with the communication network, the key-server having stored thereon the unique user identification information for a plurality of authorized users of the communication network and the secure electronic key data for use by the specific authorized user in accessing data within the network;

providing to at least a computer in communication with the communication network, a portable data storage device;

receiving user identification data indicative of an authorized user of the communication network; and,

copying from the key-server to the portable data storage device, secure electronic key data relating to the authorized user for use by the specific authorized user in accessing data within the network.

15. (Currently Amended) A method of backing up data of a key-server in communication with a communication network as defined in claim 14 wherein copying comprises:

forming a secure communication session between the key-server and the portable data storage device;

transferring the secure electronic key data relating to a specific authorized user via the secure communication session from the key-server to the portable data storage device assigned to that specific authorized user; and,

storing the transferred secure electronic key data relating to a specific authorized user within [the] memory means of the portable data storage device.

16. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein secure electronic key data specific to each of a plurality of authorized users of the communication network is stored on a separate portable data storage device assigned uniquely to one of the plurality of authorized users,

wherein the secure electronic key data of the key-server is partially stored within each portable data storage device and wherein all data within the plurality of portable data storage

devices is sufficient to restore security data to the key-server in the event of a data loss thereto.

17. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the portable data storage device includes a processor for ciphering data using the secure electronic key data stored therein and comprising:

providing cryptographic functions within the portable data storage device using the secure electronic key data stored therein.

18. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the key-server includes a processor for ciphering data using the secure electronic key data stored therein and comprising:

providing cryptographic functions within the key-server using the secure electronic key data stored therein.

19. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 18 comprising:

determining at least an available user information entry device from a plurality of known user information entry devices;

receiving unique user identification information via the at least an available user nformation entry device; and,

registering the received user identification information against secure lectronic key data for that user stored in the key-server,

wherein, when the user identification information is indicative of an authorized user, ciphering data is performed with secure electronic key data associated with the authorized user.

20. (Original) A method of backing up data of a key-server in communication with a communication network as defined in claim 16 wherein each of the plurality of

portable data storage devices are provided at each of a plurality of computers in communication with the network.

21. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 20 wherein the portable storage device comprises an interface.

22. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 16 wherein the portable storage device comprises an interface.

23. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the portable data storage device provides dedicated cryptographic functions for the at least a computer in communication with the communication network using secure electronic key data stored internal to the portable data storage device.

24. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 23 wherein the secure electronic key data stored internal to the portable data storage device are not accessible from outside of the key-server and the portable data storage device.

25. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the key-server provides dedicated cryptographic functions for the at least a computer in communication with the communication network using secure electronic key data stored internal to the key-server.

26. (Previously Presented) A method of backing up data of a key-server in communication with a communication network as defined in claim 25 wherein the secure electronic key data stored internal to the key-server are not accessible in a useable form outside of the key-server and the portable data storage device.

27. (Withdrawn) A method of authenticating an individual for allowing access to secure data or secure keys stored on a communication network when at least a secure key associated with the individual stored on a central key-server is other than available, comprising:

providing at least a computer in communication with the communication network;

determining at least an available user information entry device in communication with the computer from a plurality of known user information entry devices;

receiving user identification information via the at least an available user information entry device;

determining a presence of a portable data storage device in communication with the computer;

determining that at least a secure key associated with the individual stored on a central key-server is other than available;

when the portable data storage device is in communication with the computer, determining the availability of at least a secure key associated with the individual stored on a second key-server, the second key server being other an a central key-server, the second key server typically supporting communication with the computer; and,

upon determining that the at least a secure key associated with the individual stored on second key-server is other than available, authenticating the individual for access to at least one of the secure data and secure keys stored on the portable storage data device when the portable data storage device is in communication with the computer.

28. (Previously Presented) A method as defined in claim 27 comprising:
authenticating the individual for access to at least one of the secure data and secure keys stored on the secure portable storage data device and,

wherein the received user identification information is registered against user identification information stored in the memory means of the portable data storage device.

29. (Withdrawn) A method as defined in claim 28 comprising:

receiving identification information associated with a specific user via the at least an available user information entry device;

registering the received user identification information against security data associated

with the individual stored in the portable data storage device; and,

providing secure keys to the individual to allow access to encrypted data files that the individual has been authenticated to access.

30. (Withdrawn) A method as defined in claim 28 comprising:

receiving identification information associated with a specific user via the

at least an available user information entry device;

registering the received user identification information against security data for that user stored in the portable data storage device; and,

providing cryptographic functions within the portable data storage device using the secure keys associated with the authenticated user.

31. (original) A method as defined in claim 28 wherein when a portable data storage device is other than present prompting the user to provide a portable data storage device.

32. (Withdrawn) A method as defined in claim 28 comprising: other than when the user provides a portable data storage device authenticating the individual for access to at least one of the secure data and secure keys stored on the other than central key-server.

33. (Withdrawn) A method as defined in claim 32 comprising:

receiving unique user identification information via the at least an available user information entry device;

registering the received user identification information against security data for that user stored in the other than central key-server; and,

providing secure keys to the user to allow access to encrypted data files that the user has been authenticated to access.

34. (Withdrawn) A method as defined in claim 32 comprising:

receiving unique user identification information via the at least an available user information entry device;

registering the received user identification information against security data for that user stored in the other than central key-server; and,

providing cryptographic functions within the key-server using the secure keys associated with the authenticated user.

35. (Withdrawn) A method as defined in claim 31 wherein the portable data storage device comprises an interface.

36. (Withdrawn) A method as defined in claim 35 wherein the portable data storage device in the form of a token provides dedicated cryptographic functions for the computer using security data stored internal to the token.

37. (Withdrawn) A method as defined in claim 36 wherein the security data stored internal to the token are not accessible from outside of the token and therefore cannot be extracted or otherwise read by an unauthorized third party.

38. (Withdrawn) A method as defined in claim 32 wherein the user information entry device is a biometric information entry device.

39. (Original) A method as defined in claim 31 wherein a portable data storage device is used to provide an individual with access to a predetermined set of keys in a plurality of different locations.

40. (Original) A method as defined in claim 39 wherein the method of user authentication required at work is other than the method of user authentication required elsewhere.

41. (Original) A method as defined in claim 27 wherein the portable data storage device provides dedicated cryptographic functions for the computer using security data stored internal to the portable data storage device.

42. (Previously Presented) A method as defined in claim 41 wherein the security data stored internal to the portable data storage device are not accessible in a useable form outside of the other than central key-server and the portable data storage devices.

43. (Previously Presented) A method as defined in claim 27 wherein the key-server provides dedicated cryptographic functions for the computer using security data stored internal to the other than central key-server.

44. (Previously Presented) A method as defined in claim 43 wherein the security data stored internal to the key-server are not accessible from outside of the other than central key-server and the portable data storage devices.